IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	MDL DOCKET NO. 2800 1:17-md-2800-TWT SMALL BUSINESS CASES

OPINION AND ORDER

This is a data breach case. It is before the Court on the Defendants' Motion to Dismiss the Consolidated Small Business Class Action Complaint [Doc. 441]. For the reasons set forth below, the Defendants' Motion to Dismiss the Consolidated Small Business Class Action Complaint [Doc. 441] is GRANTED.

I. Background

On September 7, 2017, the Defendant Equifax Inc. ("Equifax") announced that it was the subject of one of the largest data breaches in history.[1] Hackers stole the personal and financial information ("the Data Breach") of nearly 150 million Americans from mid-May through the end of July 2017.[2] During this time period, Equifax failed to detect the hackers' presence in its systems, allowing the hackers to exfiltrate massive amounts of sensitive personal data

[1] Consolidated Small Business Class Action Compl. ¶ 2 [Doc. 375].

[2] *Id.*

that was in the company's custody.[3] This breach is unprecedented – it affected almost half of the entire American population.[4]

The Data Breach was also severe in terms of the type of information that the hackers were able to obtain. The hackers stole at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers.[5] This is extremely sensitive personal information. It can be used to create fake identities, fraudulently obtain loans, fraudulently obtain tax refunds, and more.[6] All of this would also destroy a consumer's credit-worthiness.[7]

Equifax is a Georgia corporation with its principal place of business in Atlanta, Georgia.[8] Equifax is the parent company of the Defendants Equifax Information Services LLC and Equifax Consumer Services LLC.[9] Both of those subsidiary companies are Georgia limited liability companies, with their

---

3 *Id.* ¶ 3.

4 *Id.* ¶ 4.

5 *Id.*

6 *Id.*

7 *Id.*

8 *Id.* ¶ 22.

9 *Id.*

principal places of business in Atlanta, Georgia.[10] The Defendants operate together as an integrated consumer reporting agency.[11]

Equifax's business model entails aggregating data relating to consumers from various sources, compiling that data into credit reports, and selling those reports to lenders, financial companies, employers, and others.[12] Credit reporting agencies are "linchpins" of the nation's financial system due to the importance of credit reports in decisions to extend credit.[13] Equifax also sells this information directly to consumers, allowing consumers to purchase their credit scores.[14] In recent years, Equifax has worked to rapidly grow its business. Recognizing the value in obtaining massive troves of consumer data, Equifax has aggressively acquired companies with the goal of expanding into new markets and acquiring new sources of data.[15] Equifax now maintains information on over 820 million individuals and 91 million businesses worldwide.[16]

---

10 *Id.* ¶¶ 23-24.

11 *Id.* ¶ 25.

12 *Id.* ¶ 42.

13 *Id.*

14 *Id.* ¶ 43.

15 *Id.* ¶ 45.

16 *Id.* ¶ 52.

Equifax recognized the importance of data security and the value of the data in its custody to cybercriminals. It observed other major, well-publicized data breaches, including those at Target, Home Depot, Anthem, and its competitor Experian.[17] Equifax held itself out as a leader in confronting such threats, offering "data breach solutions" to businesses.[18] It also acquired two identity theft protection companies, Trusted ID and ID Watchdog.[19] Equifax was also the subject of several prior data breaches. From 2010 on, Equifax suffered several different data breach incidents highlighting deficiencies in its cybersecurity protocol.[20] Given these prior breaches, cybersecurity experts concluded that Equifax was susceptible to a major data breach.[21] Analyses of Equifax's cybersecurity demonstrated that it lacked basic maintenance techniques that are highly relevant to potential data breaches.[22] However, despite these risks, Equifax did little to improve its cybersecurity practices. Equifax's leaders gave low priority to cybersecurity, spending a small fraction of the company's budget on cybersecurity.[23]

---

17 *Id.* ¶¶ 55, 68-74.

18 *Id.* ¶ 56.

19 *Id.* ¶ 55.

20 *Id.* ¶¶ 69-74.

21 *Id.* ¶ 86.

22 *Id.* ¶¶ 75-91.

23 *Id.* ¶ 125.

On March 6, 2017, a serious vulnerability in the Apache Struts software was discovered and reported.[24] This software, a popular open-source program, was used by Equifax in its consumer dispute portal website.[25] The next day, the Apache Software Foundation issued a free patch and urged all users to immediately implement the patch.[26] The Department of Homeland Security also issued warnings concerning this vulnerability.[27] Equifax internally disseminated the warning, but never implemented the patch.[28] Then, beginning on May 13, 2017, hackers were able to manipulate the Apache Struts vulnerability to access Equifax's systems; and using simple commands determined the credentials of network accounts that allowed them to access the confidential information of millions of American consumers.[29] From May 13 to July 30, 2017, the hackers remained undetected in Equifax's systems.[30] During this time, the hackers were able to steal the sensitive personally identifiable information of approximately 147.9 million American consumers.[31] The personally identifiable information

---

24 *Id.* ¶ 95.

25 *Id.* ¶¶ 92-94.

26 *Id.* ¶ 96.

27 *Id.* ¶ 97.

28 *Id.* ¶ 98.

29 *Id.* ¶ 104.

30 *Id.*

31 *Id.* ¶ 104.

that hackers obtained in the Data Breach includes names, addresses, birth dates, Social Security numbers, driver's license information, telephone numbers, email addresses, tax identification numbers, credit card numbers, credit report dispute documents, and more.[32]

On July 29, 2017, Equifax's security team noticed "suspicious network traffic" in the dispute portal.[33] The next day, the consumer dispute portal was deactivated and taken offline. On July 31, 2017, Equifax's CEO Richard Smith was informed of the breach.[34] On August 2, 2017, Equifax informed the Federal Bureau of Investigation about the Data Breach, and retained legal counsel to guide its investigation.[35] Equifax also hired cybersecurity firm Mandiant to investigate the suspicious activity.[36] On September 7, 2017, seven weeks after discovering suspicious activity, Equifax publicly disclosed the Data Breach in a press release.[37] Experts have since opined that the Data Breach was the result of weak cybersecurity measures and a low priority for data security.[38]

---

[32] *Id.* ¶ 4.

[33] *Id.* ¶¶ 105-06.

[34] *Id.* ¶ 107.

[35] *Id.* ¶ 110.

[36] *Id.*

[37] *Id.* ¶ 136.

[38] *Id.* ¶¶ 183-89.

The Plaintiffs are ten "small businesses," including corporations and limited liability companies.[39] In contrast to the Putative Consumer Class Action, the Small Business Plaintiffs here seek to represent a class of small businesses, which are separate and distinct legal entities. These Plaintiffs allege that they rely upon the personal creditworthiness of their owners to obtain and maintain credit, and seek to recover for their own injuries resulting from the Data Breach. The Small Business Plaintiffs allege that they have been harmed by having to take measures to combat the risk of identity theft and by expending time and effort to monitor their credit and identity.[40] The Plaintiffs assert claims for negligence, negligence per se, violation of the Georgia Fair Business Practices Act, unjust enrichment, and recovery of litigation expenses under O.C.G.A. § 13-6-11. The Plaintiffs also seeks declaratory and injunctive relief. The Defendants now move to dismiss.

II. Legal Standard

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a "plausible" claim for relief.[41] A complaint may survive a motion to dismiss for failure to state a claim, however, even if it is "improbable" that a plaintiff would be able to prove those facts; even

---

39 *Id.* ¶¶ 12-22.

40 *Id.* ¶¶ 12-21.

41 *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1949 (2009); FED. R. CIV. P. 12(b)(6).

if the possibility of recovery is extremely "remote and unlikely."[42] In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff.[43] Generally, notice pleading is all that is required for a valid complaint.[44] Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon which it rests.

III. Discussion

A. Choice of Law

First, the Court concludes that Georgia law governs this case. This case is before the Court based on diversity jurisdiction. The Court therefore looks to Georgia's choice of law requirements to determine the appropriate rules of decision.[45] Georgia follows the traditional approach of *lex loci delecti* in tort cases, which generally applies the substantive law of the state where the last

---

[42] *Bell Atlantic v. Twombly*, 550 U.S. 544, 556 (2007).

[43] *See Quality Foods de Centro America, S.A. v. Latin American Agribusiness Dev. Corp., S.A.*, 711 F.2d 989, 994-95 (11th Cir. 1983); *see also Sanjuan v. American Bd. of Psychiatry and Neurology, Inc.*, 40 F.3d 247, 251 (7th Cir. 1994) (noting that at the pleading stage, the plaintiff "receives the benefit of imagination").

[44] *See Lombard's, Inc. v. Prince Mfg., Inc.*, 753 F.2d 974, 975 (11th Cir. 1985), *cert. denied*, 474 U.S. 1082 (1986).

[45] *Frank Briscoe Co., Inc. v. Ga. Sprinkler Co., Inc.*, 713 F.2d 1500, 1503 (11th Cir.1983) ("A federal court faced with the choice of law issue must look for its resolution to the choice of law rules of the forum state.").

event occurred necessary to make an actor liable for the alleged tort.[46] Usually, this means that the "law of the place of the injury governs rather than the law of the place of the tortious acts allegedly causing the injury."[47] However, there is an exception when the applicable law of the foreign state is the common law. "[T]he application of another jurisdiction's laws is limited to statutes and decisions construing those statutes. When no statute is involved, Georgia courts apply the common law as developed in Georgia rather than foreign case law."[48] The Plaintiffs identify no foreign statutes that govern their common law claims, therefore the Court will apply Georgia law.[49]

---

[46] *Dowis v. Mud Slingers, Inc.*, 279 Ga. 808, 816 (2005); *Int'l Bus. Machines Corp. v. Kemp*, 244 Ga. App. 638, 640 (2000).

[47] *Mullins v. M.G.D. Graphics Sys. Grp.*, 867 F. Supp. 1578, 1581 (N.D. Ga. 1994).

[48] *In re Tri-State Crematory Litig.*, 215 F.R.D. 660, 677 (N.D. Ga. 2003) (internal quotations omitted). The Georgia Supreme Court has recently reaffirmed this exception. *See Coon v. The Med. Ctr., Inc.*, 300 Ga. 722, 729 (2017) ("In the absence of a statute, however, at least with respect to a state where the common law is in force, a Georgia court will apply the common law as expounded by the courts of Georgia.").

[49] The Plaintiffs argue that Georgia law should apply unless the Court decides "that Georgia law is adverse to the common law claims of the national class pled in the Complaint, in which case it will be necessary to consider the common law of each state applicable to the proposed alternative, state-specific classes." Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 7. However, the Plaintiffs cite no authority for such a proposition. The Court concludes that Georgia law will govern this case.

B. Standing

The Defendants contend that the Plaintiffs lack Article III standing.[50] In order to establish standing under Article III, a plaintiff must show an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[51] The Supreme Court has held that "threatened injury must be *certainly impending* to constitute injury in fact, and that allegations of *possible* future injury are not sufficient."[52] The Supreme Court has also noted, however, that standing can be "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[53] The Defendants contend that the Plaintiffs lack standing because they do not allege that their information was compromised during the Data Breach, but instead only that their owners' personal information was compromised. This "chain of events" to cause injury to the Plaintiffs, according to the Defendants, is too attenuated to confer standing.

First, the Defendants contend that the Plaintiffs have not adequately alleged that they have suffered a cognizable injury-in-fact.[54] A "plaintiff must

---

50 Defs.' Mot. to Dismiss, at 10.

51 *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013).

52 *Id.*

53 *Id.* at 1150 n.5.

54 Defs.' Mot. to Dismiss, at 12.

allege that he has suffered a 'concrete' injury particular to himself."[55] The Plaintiffs do not allege that their information was compromised during the Data Breach. Instead, they merely allege that their owners' Personal Information was compromised. The Small Business Plaintiffs allege that because their owners' Personal Information was compromised, the breach has "jeopardized" "the creditworthiness and continued operations" of the Small Business Plaintiffs and that they have "reasonably incurred costs . . . based on the substantial risk of harm from the breach."[56] Therefore, following *Spokeo*, the Small Business Plaintiffs have failed to plead facts showing an essential element of standing, injury to themselves rather than another.[57] The owners of the Small Business Plaintiffs chose to do business as corporations or limited liability companies. The Small Business Plaintiffs have offered no authority that this legal distinction should be ignored in the standing analysis. The owners of the Small Business Plaintiffs may seek recovery of their damages in the Consumer Class action. They are not entitled to a second recovery here.

Second, the injury must be "actual or imminent, not conjectural or hypothetical."[58] The Defendants contend that the Plaintiffs' alleged injuries are

---

[55] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1552 (2016).

[56] Consolidated Small Business Class Action Compl. ¶¶ 12-21.

[57] *See Spokeo, Inc.*, 136 S. Ct. at 1548 ("For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'").

[58] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

too attenuated and too speculative and conjectural.[59] The Defendants argue that the Plaintiffs' alleged injuries fall into two categories: the "increased risk" of future harm to their creditworthiness and business operations, and "voluntary" costs to mitigate that alleged risk.[60] But to establish any actual harm from that purported risk, the Small Business Plaintiffs would have to plead, and ultimately prove, the following chain of events:

- The owner's PII was compromised in the Equifax data breach;
- The owner's PII was obtained by some criminals as a result of the Equifax data breach and then misused by those criminals;
- The owner's credit was directly impacted by the criminals' misuse of his or her PII (as opposed to any other factor among a multitude of factors that can affect a consumer's credit);
- The Small Business Plaintiff thereafter attempted to rely on the owner's credit for its own "creditworthiness and continued operations"; and
- The Small Business Plaintiff's "creditworthiness [or] continued operations" were harmed—e.g., a denied loan application or increased interest rate—as a direct result of the owner's damaged credit (as opposed to any other element taken into consideration for the extension of business credit).[61]

These alleged injuries are too speculative because any break in the attenuated causal chain would result in the injuries not occurring, and also because the

---

[59] Defs.' Mot. to Dismiss, at 12-14.

[60] *Id.* at 13.

[61] *Id.* at 13-14.

"risk of harm" resulting from compromised personal information itself is too uncertain.[62]

Furthermore, the Court concludes that the Plaintiffs have not alleged a substantial risk of harm that is sufficient to confer standing. In *Clapper*, the Supreme Court noted that standing can be "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[63] In both *Arby's* and *Home Depot*, this Court concluded that allegations that a plaintiff incurred costs mitigating the substantial risk of harm from a data breach were sufficient to confer standing.[64] However, in those cases, credit card data belonging to the consumers and the financial institutions had been stolen. That was an imminent injury because the data could be used immediately to make fraudulent credit charges. In contrast,

---

[62] *Clapper*, 133 S. Ct. at 1148 ("[R]espondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.").

[63] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1150 n.5 (2013).

[64] *See In re Arby's Restaurant Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441, at *11 (N.D. Ga. Mar. 5, 2018) ("The Consumer Plaintiffs' allegations that they suffered monetary losses related to fraudulent charges—unauthorized charges on their accounts, theft of their personal financial information, and costs associated with detection and prevention of identity theft—are sufficient to survive a motion to dismiss."); *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-md-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) ("These injuries are not speculative and are not threatened future injuries, but are actual, current, monetary damages. Additionally, any costs undertaken to avoid future harm from the data breach would fall under footnote 5 of *Clapper*, specifically as reasonable mitigation costs due to a substantial risk of harm.").

a chain of events would need to occur for the Small Business Plaintiffs to suffer their purported injuries. This does not constitute a "substantial risk" of an "imminent injury."

The Defendants also argue that "voluntary costs" taken in response to the Data Breach cannot establish standing.[65] According to the Defendants, the Plaintiffs cannot "manufacture" standing by taking on voluntary costs. Unfortunately, in this digital age, the Small Business Plaintiffs have alleged nothing more than the exercise of ordinary due diligence in monitoring their creditworthiness. It is equally plausible that they would have done the same things with or without the Equifax Data Breach. Therefore, the Court concludes that the Small Business Plaintiffs have not adequately alleged an injury-in-fact to them. The Motion to Dismiss should be granted for lack of Article III standing.

C. Economic Loss Doctrine

The Defendants also argue that the economic loss doctrine bars the Plaintiffs' tort claims.[66] "The 'economic loss rule' generally provides that a contracting party who suffers purely economic consequences must seek his remedy in contract and not in tort."[67] "Under the economic loss rule, a plaintiff

---

[65] Defs.' Mot. to Dismiss, at 15.

[66] Defs.' Mot. to Dismiss, at 39.

[67] *General Elec. Co. v. Lowe's Home Centers, Inc.*, 279 Ga. 77, 78 (2005).

can recover in tort only those economic losses resulting from injury to his person or damage to his property; a plaintiff cannot recover economic losses associated with injury to the person or damage to the property of another."[68] As discussed above, the injury here was not to the Small Business Plaintiffs but to their owners. Therefore, the claim of the Small Business Plaintiffs is barred by the economic loss rule. Where, however, "an independent duty exists under the law, the economic loss rule does not bar a tort claim because the claim is based on a recognized independent duty of care and thus does not fall within the scope of the rule."[69] "It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information[.]"[70] But that duty extends to the consumer, not to anyone in the world (a spouse, a child, a friend, a partner) who might possibly want to take advantage of the consumer's good credit. Imposing such a duty as to the consumer whose personal information is compromised serves the purposes of tort law: compensation and deterrence. The Small Business Plaintiffs offer no precedent for expanding that duty to them. In *Home Depot,* the financial institutions were not relying upon the compromise of their customers'

---

68 *Id.*

69 *Liberty Mut. Fire Ins. Co. v. Cagle's, Inc.*, No. 1:10-cv-2158-TWT, 2010 WL 5288673, at *3 (N.D. Ga. Dec. 16, 2010).

70 *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017).

information. The financial institution plaintiffs in *Home Depot* were card issuers whose payment card data was stolen. The Small Business Plaintiffs are seeking to recover economic losses due to injury to others. Therefore, their claims are barred by the economic loss rule.

IV. Conclusion

For the reasons stated above, the Defendants' Motion to Dismiss the Consolidated Small Business Class Action Complaint [Doc. 441] is GRANTED.

SO ORDERED, this 28 day of January, 2019.

/s/Thomas W. Thrash
THOMAS W. THRASH, JR.
United States District Judge